Payment Tracers (PT) – Privacy Impact Assessment (PIA)

PIA Approval Date: November 17, 2009

System Overview

The purpose of the Payment Tracers (PT) application is to allow users in the Hardcore Payment Tracers (HCPT) Units in the Accounting areas to: Research payments from Error Resolution (ERS) processing using taxpayer identification number (TIN) changes; Control Payment Tracers cases; Submit document locator numbers (DLNs) electronically to Enterprise Computing Center – Martinsburg (ECC-MTB) for research against the Master File; View the returned ECC-MTB DLN research data; and Print various reports used by the HCPT Units.

Systems of Records Notice (SORN):

- Treasury/IRS 36.003 General Personnel and Payroll Records
- Treasury/IRS 34.037 IRS Audit Trail and Security Records System
- Treasury/IRS 26.019 Taxpayer Delinquent Accounts (TDA) Files
- Treasury/IRS 24.046 CADE Business Master File (BMF)
- Treasury/IRS 24.030 CADE Individual Master File (IMF)
- Treasury/IRS 00.001 Correspondence Files (including Stakeholder Relationship files) and Correspondence Control Files

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer:
  - Taxpayer Identification Number (TIN)
  - Original TIN
  - New TIN
  - Name control
  - Document Locator Number (DLN)
  - DLN type
  - Transmit date
  - Processing years
  - Control day
  - Control date
  - Payment amount
  - Payment date
  - Bank name
  - Tax period
  - Master File Tax (MFT)
  - Cycle
  - Transaction date
  - Transaction code

B. Employee – Payment Tracers contain employee's:
  - Login identification number
  - First name
  - Last name

- Phone number
- The site that they belong (work site) of the employee working the case.

C. Audit Trail Information – The Payment Tracers application is located at ECC-MEM, and resides on two SUN UNIX servers: TS00075B and TS00054 (which will become TS00112 towards the end of the 2009 calendar year). The application collects the employees' login id and login date and time.

D. Other – The control date and comments about the case are entered by the Internal Revenue Service (IRS) employee working on the case.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS – Obtained from Error Resolution System (ERS) runs files ERS1101 and ERS0505 and Master File extracts:

- Taxpayer Identification Number (TIN)
- Original TIN
- New TIN
- Name control
- Document Locator Number (DLN)
- DLN type
- Transmit date
- Processing years
- Control day
- Payment amount
- Payment date
- Tax period
- Master File Tax (MFT)
- Cycle
- Transaction date
- Transaction code

B. Taxpayer – Obtained from the taxpayer:

- Bank name

C. Employee – Obtained from the employee working the case:

- Employee number
- Control Date
- Case Comments

3. Is each data item required for the business purpose of the system? Explain.
Yes. Each data item is required to identify and locate the correct payments.

4. How will each data item be verified for accuracy, timeliness, and completeness?
The Payment Tracer application performs limited field validation on data entered by the IRS employee. All other information input into the Payment Tracer application is provided from other IRS systems. Error Resolution Runs and Master File extracts have their own built-in processes which validate the information before it is sent into the Payment Tracer application.

The Payment Tracer application parses and verifies the data while loading it into the Payment Tracer database tables.

5. Is there another source for the data? Explain how that source is or is not used.
No. There is no other source of data for PT.

6. Generally, how will data be retrieved by the user?
The data is generally retrieved when an employee enters the DLN into the system.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. The data is also retrievable by entering the TIN, Social Security Number (SSN) or Employer Identification Number (EIN) into the system.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Users and Managers in the Payment Tracers Units (that work the case at the site) have access to data in the system. Access to the data is determined by the Manager based on a user’s position and need-to-know basis as part of his/her official duties.

The types of transactions that users can perform include:

- **Tax Examiner** – Has privilege access to only the first screen (DLN Research screen) and input data into the system. Has Basic Read and Write permission to certain parts of the application
- **Clerk (Customer Representative)** – Has privilege access and does work of Payment Tracer Unit and 'tax examiner.' Has Read and Write permission to certain parts of the system, with more permission than Tax Examiner
- **Lead (Manager)** – Oversees users of Payment Tracer Unit, 'clerk' and 'tax examiner' privilege. The Manager/Lead has the ability to create, modify, or alter the roles/permissions of their users. Manager/Lead also has the ability to review the activities of their users in the database table. The Manager/Lead only sees users of their site and cannot modify or review users in other locations
- **Administrator** – privilege is only for the Online 5081 (OL5081) “PTADMIN” group. Their main and only purpose is to add/delete users of the application. Having 'administrator' privilege also includes the other lower privileges, but no Payment Tracers work should be performed by an 'administrator'

9. How is access to the data by a user determined and by whom?
The user’s manager/lead determines the users’ access while the PT administrators provide a second level of approval prior to granting system access to the users. PT access is initiated through the OL5081 process:

- The manager will request that users be granted access to the application, added, or deleted via OL5081, Information System User Registration/Change Request. A user’s access to the data terminates when it is no longer a required part of his/her official duties.
- Criteria, procedures, controls, and responsibilities regarding access are documented in the Information System Security Rules on OL5081.

- Level of access to the data is determined by the Manager based on a user’s position and need-to-know.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
Yes. From Unisys Mainframe (MITS-23 GSS): Error Resolution System runs ERS05 and ERS11 provide input into LF346 which checks and sends any TIN changes via File Transfer Protocol (FTP) daily to Payment Tracer. It sends:

- DLN,
- Processing Year,
- Control day,
- original TIN,
- new TIN

From IBM Mainframe IAP (MITS-20 GSS) which is an acronym for ICS/ACS/PRINT which is an acronym for Integrated Collection System (ICS) / Automated Collection System (ACS) / Printing (PRINT): IAP takes Payment Tracer DLN input and extracts matches and provides via File Transfer Protocol (FTP) monthly to Payment Tracer. It sends:

- DLN,
- TIN,
- Name control,
- Tax period,
- Master File Type (MFT),
- Cycle,
- Transaction date,
- Transaction code,
- Control date

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes. Error Resolution and Master File are Unisys runs. The Unisys System is approved under the Service Center Support System PIA.

IBM Mainframe IAP (MITS-20 GSS):

- Authority To Operate (ATO) (September 28, 2007)
- PIA Approval (October 18, 2009)

12. Will other agencies provide, receive, or share data in any form with this system?
No. No other agencies provide, receive, or share data in any form with Payment Tracers.

<u>Administrative Controls of Data</u>

13. What are the procedures for eliminating the data at the end of the retention period?
Payment Tracers follows the record control schedule: Record management, record control schedule for tax administration – Wage and Investment records: IRM 1.15.29, Exhibit 1, Number 185.

14. Will this system use technology in a new way?
No. Payment Tracers will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. Payment Tracers is not used to identify or locate individuals or groups. The system is used to locate payments made by taxpayers.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No. Payment Tracers does not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. Payment Tracers is designed to facilitate a required manual process. The system cannot be used by the IRS to treat taxpayers, employees, or others, differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
No. The application is used to identify lost, missing, or misapplied payments. With the help of this program, taxpayers' accounts can be corrected and made whole before any harm or action is taken by the IRS against the taxpayers.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
The application's interface is web-based, and is only accessible to IRS Hard Core Payment Tracer Function users. The system does not use any cookies or tracking devices other than the login name that allows users access to the application.

View other PIAs on IRS.gov